

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-082963

(43)Date of publication of application : 21.03.2000

(51)Int.Cl.

H03M 7/00
G11B 20/10

(21)Application number : 10-252299

(71)Applicant : M KEN:KK

(22)Date of filing : 07.09.1998

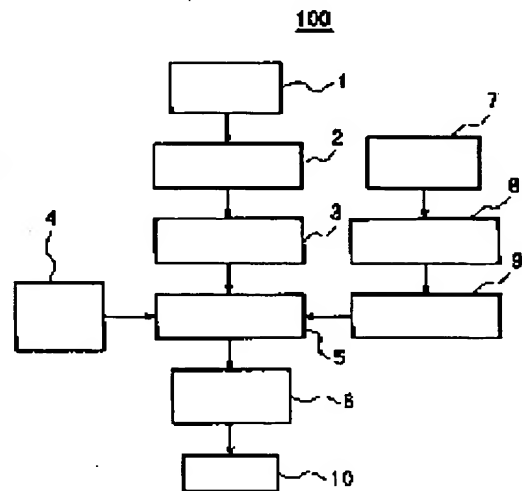
(72)Inventor : SUZUKI AKIRA
ISHIYAMA KUMIKO
SAWATO SHUSAKU

(54) DIGITAL DATA WORK PROCESSING METHOD, DIGITAL DATA WORK PROCESSOR AND RECORDING MEDIUM RECORDING DIGITAL DATA WORK PROCESSING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To bury security data in a digital data work based on a simple technological constitution and to provide the processing method of a digital data work, which avoid erroneous judgment, data destruction or with high secrecy against a third party.

SOLUTION: A digital data work storage means 1, a security data storage means 7 are provided. A parameter selection means 2 selecting a parameter in a work storage means 1, a bit position extraction means 3 burying security data is buried from the selected parameter in accordance with a prescribed rule, an algorithm storage means 4 storing an algorithm where security data is buried, a bit data extraction means 9 extraction individual bit values from security data, a security data burying means 5 burying a security data bit value in a bit position where extracted security data is to be buried and a digital data author output means 6 outputting a digital data work where security data is buried are installed and a digital data work processor 100 is constituted.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2000-82963

(P2000-82963A)

(43)公開日 平成12年3月21日(2000.3.21)

(51)Int.Cl.⁷

識別記号

F I

特マコード(参考)

H 0 3 M 7/00

H 0 3 M 7/00

5 D 0 4 4

G 1 1 B 20/10

G 1 1 B 20/10

H 5 J 0 6 4

審査請求 未請求 請求項の数22 O L (全 16 頁)

(21)出願番号

特願平10-252299

(22)出願日

平成10年9月7日(1998.9.7)

(71)出願人 597108822

株式会社エム研

東京都渋谷区元代々木町31番1号

(72)発明者 鈴木 晶

東京都渋谷区西原1-36-1 MS西原ビル306室

(72)発明者 石山 久美子

東京都調布市市布田5-34-1 アルジェント調布式番館201号

(72)発明者 澤戸 周作

千葉県千葉市磯辺7-3-16

(74)代理人 100071755

弁理士 斉藤 武彦 (外1名)

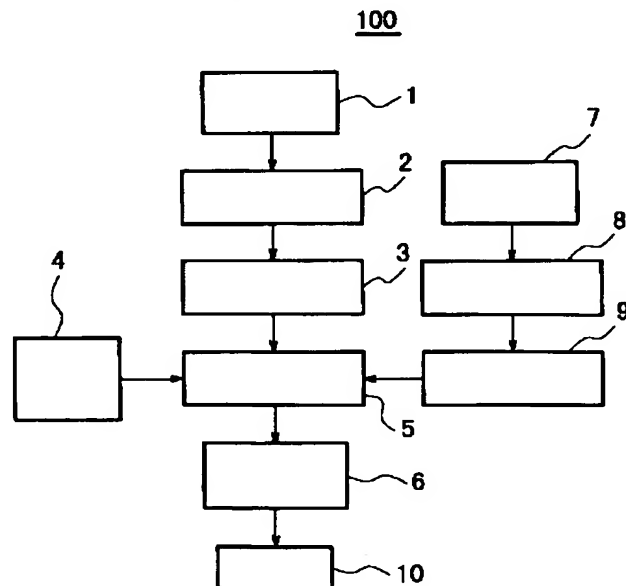
最終頁に続く

(54)【発明の名称】 デジタルデータ著作物処理方法、デジタルデータ著作物処理装置、デジタルデータ著作物処理プログラムを記録した記録媒体

(57)【要約】

【課題】 簡易な技術構成に基づき、セキュリティデータをデジタルデータ著作物に埋め込むと共に、誤判断、データ破壊、或いは第3者に対する秘匿性の高いデジタルデータ著作物の処理方法を提供する。

【解決手段】 デジタルデータ著作物記憶手段1、セキュリティデータ記憶手段7、著作物記憶手段1内の著作物からパラメータを選択するパラメータ選択手段2、選択されたパラメータから所定の規則に従ってセキュリティデータを埋込むビット位置抽出手段3、セキュリティデータを埋込むアルゴリズムを記憶するアルゴリズム記憶手段4、セキュリティデータから個々のビット値を抽出するビットデータ抽出手段9、抽出されたセキュリティデータを埋め込むべきビット位置に対して、セキュリティデータビット値を埋め込むセキュリティデータ埋め込み手段5、及びセキュリティデータを埋め込んだデジタルデータ著作物を出力するデジタルデータ著作物出力手段6 とからなるデジタルデータ著作物の処理装置100。



【特許請求の範囲】

【請求項1】 デジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティーデータを埋め込むに際し、当該デジタルデータ著作物を構成するデジタルデータ群から少なくとも1つのパラメータを選択し、当該選択されたパラメータに於て、当該パラメータを構成する当該デジタルデータから、予め定められた規則に従って、当該セキュリティーデータを埋め込むビットを含むデータ位置を当該パラメータが配列されている時間軸若しくは走査方向軸に沿って順次選択抽出した後、当該選択抽出された個々のビットのそれぞれに対して、当該埋め込むべきセキュリティーデータを構成するビット列の各ビットデータを順次に埋め込む事の特徴とするデジタルデータ著作物の処理方法。

【請求項2】 当該デジタルデータ著作物を構成するデジタルデータ群から一つのパラメータが選択され、当該選択されたパラメータを構成するデジタルデータのビット列からなるデータ位置に対して、当該時間軸若しくは走査方向軸に沿って予め定められた規則に従って、当該セキュリティーデータを埋め込むべきデータ位置を選択抽出する事の特徴とする請求項1記載のデジタルデータ著作物の処理方法。

【請求項3】 当該デジタルデータ著作物を構成するデジタルデータ群から複数種類のパラメータが選択され、当該時間軸若しくは走査方向軸に沿って、当該セキュリティーデータを埋め込むビット位置を当該選択された複数種のパラメータ間で変化させる事の特徴とする請求項1記載のデジタルデータ著作物の処理方法。

【請求項4】 当該時間軸若しくは走査方向軸に沿って、当該セキュリティーデータを埋め込むデジタルデータ位置を選択抽出するに際して、予め定められた規則に従って、当該選択された複数種のパラメータ群の中から一つのパラメータを当該時間軸若しくは走査方向軸に沿って順次に選択するものである事の特徴とする請求項3記載のデジタルデータ著作物の処理方法。

【請求項5】 当該選択された当該セキュリティーデータを埋め込むべきビット位置に、当該セキュリティーデータを構成するビット列の所定のビット値が埋め込まれるものである事の特徴とする請求項1乃至4の何れかに記載のデジタルデータ著作物の処理方法。

【請求項6】 当該セキュリティーデータを構成するビット列の所定のビット値を当該選択されたパラメータに於ける予め選択抽出された、データ位置に有る複数のビット列で構成されたデータ部に対して埋め込むに際し、当該パラメータデータ部を予め定められたアルゴリズムに従って埋込処理するものである事の特徴とする請求項1乃至4の何れかに記載のデジタルデータ著作物の処理方法。

【請求項7】 当該アルゴリズムは、当該パラメータを構成するデジタルデータを当該デジタルデータの通常の

変化の量よりも広い間隔で量子化するものである事の特徴とする請求項6記載のデジタルデータ著作物の処理方法。

【請求項8】 当該量子化手段は、モジュロX（X=任意の整数）である事の特徴とする請求項7記載のデジタルデータ著作物の処理方法。

【請求項9】 当該セキュリティーデータは、少なくとも、固定ビットパターン部、セキュリティーデータビット部及びエラー検出ビット部とから構成されている事の特徴とする請求項1乃至8の何れかに記載のデジタルデータ著作物の処理方法。

【請求項10】 当該デジタルデータ著作物は、画像データである事の特徴とする請求項1乃至9の何れかに記載のデジタルデータ著作物の処理方法。

【請求項11】 当該デジタルデータ著作物は、音楽データである事の特徴とする請求項1乃至9の何れかに記載のデジタルデータ著作物の処理方法。

【請求項12】 当該音楽データは、MIDI（Music Instrumental Digital Interface）の規格により構成されているデータである事の特徴とする請求項11に記載のデジタルデータ著作物の処理方法。

【請求項13】 デジタルデータ著作物記憶手段、セキュリティーデータ記憶手段、当該デジタルデータ著作物記憶手段に記憶されているデジタルデータ著作物のデジタルデータからパラメータを選択するパラメータ選択手段、当該選択されたパラメータから予め定められた規則に従ってセキュリティーデータを埋め込む複数のビットデータで構成されたデジタルデータのデータ位置及びそのデータ値を抽出する埋め込み位置及び埋め込みデータ抽出手段、セキュリティーデータを埋め込むに際してのアルゴリズムを記憶するアルゴリズム記憶手段、当該セキュリティーデータ記憶手段から抽出された個々のセキュリティーデータに対して固定ビットパターン及びエラー検出ビットを付加するデータ付加手段、当該データ付加手段から出力されるセキュリティーデータのビット列から個々のビット値を抽出するセキュリティーデータビットデータ抽出手段、当該埋め込み位置及び埋め込みデータ抽出手段によって抽出された当該セキュリティーデータを埋め込むべきビット位置群及びビットデータに対して、当該セキュリティーデータビットデータ抽出手段からの情報に応答して、当該アルゴリズム記憶手段に記憶されたアルゴリズムに従って、所定のセキュリティーデータビット値が埋め込まれる様に埋込処理を実行するセキュリティーデータ埋め込み手段、及び当該セキュリティーデータを埋め込んだデジタルデータ著作物を出力するデジタルデータ著作物出力手段とから構成されている特徴とするデジタルデータ著作物の処理装置。

【請求項14】 デジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティーデータを埋め込むに際し、セキュリティーデータを埋め込むべきデジ

タルデータ著作物を用意する第1の工程、
当該デジタルデータ著作物を構成するデジタルデータ群の中から少なくとも1つのパラメータを選択する第2の工程、
当該選択されたパラメータを構成する当該デジタルデータ群から、予め定められた規則に従って、当該セキュリティデータを埋め込むべきデータ位置を当該パラメータが配列されている時間軸若しくは走査方向軸に沿って順次選択抽出する第3の工程、
当該セキュリティデータを埋め込む為に選択抽出されたデータ位置の個々のビットデータ或いは選択されたデータ位置群のビットデータを記憶する第4の工程、
予め定められたセキュリティデータを用意する第5の工程、
当該セキュリティデータに対して予め定められた固定ビットパターン及びエラー検出ビットを付加する第6の工程、
当該固定ビットパターン及びエラー検出ビットを含むセキュリティデータのビット列から個々のビットデータを順次を選択する第7の工程、
当該セキュリティデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ或いは選択されたビット位置群のビットデータに対して、当該選択された個々のセキュリティデータのビット列のビットデータに応答して、当該アルゴリズムを介して、所定のセキュリティデータビット値が埋め込まれる様に埋込処理を実行する第8の工程、及び当該埋込処理され所定のセキュリティデータビット値が埋め込まれデジタルデータ著作物を出力する第9の工程とから構成されている事の特徴とするデジタルデータ著作物の処理方法。

【請求項15】 デジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティデータを埋め込むに際し、セキュリティデータを埋め込むべきデジタルデータ著作物を用意する第1の工程、
当該デジタルデータ著作物を構成するデジタルデータ群の中から少なくとも1つのパラメータを選択する第2の工程、
当該選択されたパラメータを構成する当該デジタルデータ群から、予め定められた規則に従って、当該セキュリティデータを埋め込むべきデータ位置或いはデータ位置群を当該パラメータが配列されている時間軸若しくは走査方向軸に沿って順次選択抽出する第3の工程、
当該セキュリティデータを埋め込む為に選択抽出されたデータ位置の個々のビットデータ或いは選択されたデータ位置群のビットデータを記憶する第4の工程、
予め定められたセキュリティデータを用意する第5の工程、
当該セキュリティデータに対して予め定められた固定ビットパターン及びエラー検出ビットを付加する第6の工程、

当該固定ビットパターン及びエラー検出ビットを含むセキュリティデータのビット列から個々のビットデータを順次を選択する第7の工程、
当該セキュリティデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ或いは選択されたビット位置群のビットデータに対して、当該選択された個々のセキュリティデータのビット列のビットデータに応答して、当該アルゴリズムを介して、所定のセキュリティデータビット値が埋め込まれる様に埋込処理を実行する第8の工程、及び当該埋込処理され所定のセキュリティデータビット値が埋め込まれデジタルデータ著作物を出力する第9の工程とから構成されているデジタルデータ著作物の処理方法をコンピュータに実行させる為のプログラムを記録した記録媒体。

【請求項16】 セキュリティデータが埋め込まれたデジタルデータから当該埋め込まれている当該セキュリティデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択し、当該パラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、順次に且つ予め定められた規則に従って当該デジタルデータ群から所定のビットデータ或いは複数のビットデータからなるデータ位置群を抽出した後、当該選択抽出された当該データ位置或いは当該データ位置群を構成するデータのそれぞれに順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換後、当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティデータを表わすビットデータ値列と比較判定し、両者が一致したセキュリティデータを出力する様に構成されている事の特徴とするデジタルデータ著作物処理方法。

【請求項17】 当該デジタルデータ著作物を構成するデジタルデータ群から一つのパラメータが選択され、当該選択されたパラメータを構成するデジタルデータのビット列からなるデータ位置を、当該時間軸若しくは走査方向軸に沿って予め定められた規則に従って、選択抽出する事の特徴とする請求項16記載のデジタルデータ著作物の処理方法。

【請求項18】 当該デジタルデータ著作物を構成するデジタルデータ群から複数種類のパラメータが選択され、予め定められた規則に従って、当該選択された複数種のパラメータ群の中から一つのパラメータを当該時間軸若しくは走査方向軸に沿って順次に選択すると同時に、当該選択されたそれぞれのパラメータを構成するデジタルデータのビット列からなるデータ位置を、当該時間軸若しくは走査方向軸に沿って予め定められた規則に従って、選択抽出する事の特徴とする請求項16記載のデジタルデータ著作物の処理方法。

【請求項19】 セキュリティデータが埋め込まれているデジタルデータ著作物を格納しているデジタルデー

タ著作物記憶手段、セキュリティーデータ記憶手段、当該デジタルデータ著作物記憶手段に記憶されているセキュリティーデータが埋め込まれているデジタルデータ著作物のデジタルデータから予め定められたパラメータを選択するパラメータ選択手段、当該選択されたパラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、予め定められた規則に従って当該デジタルデータ群からビットデータ或いは複数のビットデータからなるビットデータ位置群を順次を選択抽出するデータ抽出手段、セキュリティーデータを埋め込むに際してのアルゴリズムを記憶するアルゴリズム記憶手段、当該データ抽出手段から抽出された個々の当該ビットデータ或いは複数のビットデータからなるビットデータからなるデータ位置群に、当該アルゴリズムを適用して新たなビットデータ値列に変換するデータ変換手段、当該新たなビットデータ値列を、予めセキュリティーデータ記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較判定する手段、及び両者が一致した場合に、一致したセキュリティーデータを出力するセキュリティーデータ出力手段とから構成されている事の特徴とするデジタルデータ著作物処理装置。

【請求項20】 セキュリティーデータが埋め込まれたデジタルデータから当該埋め込まれている当該セキュリティーデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択する第1の工程、

当該選択されたパラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、順次に且つ予め定められた規則に従って当該デジタルデータから所定のビットデータ或いは複数のビットデータからなるデータ位置群を抽出する第2の工程、

当該選択抽出された当該ビットデータ或いは当該ビットデータからなるデータ位置群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換する第3の工程、

当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較し両者が一致するか否かを判断する第4の工程、

両者が一致した場合に、当該一致したセキュリティーデータを出力する第5の工程、

とから構成されている事の特徴とするデジタルデータ著作物処理方法。

【請求項21】 当該パラメータの選択する第1の工程に於いて、一つのデジタルデータ著作物のデジタルデータから複数種のパラメータを選択し、当該選択された複数種のパラメータ群の中から一つのパラメータを当該時間軸若しくは走査方向軸に沿って順次を選択すると同時

に、当該選択されたそれぞれのパラメータを構成するデジタルデータのビット列から、当該時間軸若しくは走査方向軸に沿って予め定められた規則に従って、当該ビットデータ或いは複数のビットデータからなるデータ位置群を選択抽出する操作が実行されるものである事の特徴とする請求項20記載のデジタルデータ著作物処理方法。

【請求項22】 セキュリティーデータが埋め込まれたデジタルデータから当該埋め込まれている当該セキュリティーデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択する第1の工程、

当該選択されたパラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、順次に且つ予め定められた規則に従って当該デジタルデータから所定のビットデータ或いは複数のビットデータからなるビットデータからなるデータ位置群を抽出する第2の工程、

当該選択抽出された当該データ位置群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換する第3の工程、

当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較し両者が一致するか否かを判断する第4の工程、

両者が一致した場合に、当該一致したセキュリティーデータを出力する第5の工程、とから構成されているデジタルデータ著作物の処理方法をコンピュータに実行させる為のプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルデータ著作物の処理方法及びデジタルデータ著作物処理装置等に関するものであり、更に詳しくは、画像データ及び音楽データを主とするデジタルデータ著作物に対する不正なコピーを有効に防止する為のデジタルデータ著作物の処理方法及びデジタルデータ著作物処理装置に関するものである。

【0002】

【従来の技術】従来より、テープ、ディスク等の任意の記録媒体に記録されているデジタル音声データ、楽音データ等の音声データが、当該記録媒体が一旦市場で販売された後は、同音声データの著作権者の同意を得ることなく、勝手にコピーされ、係る不正コピーが、大量に安価に販売されていることから、著作権者の権利が不当に侵害され、当著作権者が大幅な損害を被っているのが現状である。

【0003】然も、現在では、係る不正なコピーを有効に防止する手段は、実質的にはなく、法律上からも証拠の確認が難しいので、係る不正なコピー、海賊版を訴追

する事が難しい状態にある。係る、音声データの不正なコピーを防止する方法には多くの方法が、提案されているが、再生音の音質が低下するとか画像の画質が低下する等の問題があり、実用にはなっていないのが現状である。

【0004】そこで、この問題を改善する為に、デジタル画像或いは、デジタル音声データに、その画像データ或いは音声データの著作権者、または、その実施権者が、自らの意思によって、販売を許可した真正な画像データ或いは音声データであることを示す、デジタルビットデータから構成された暗号、署名データ等のセキュリティデータを、当該音声データそのものに聴覚的に影響のないように埋め込み、その音声データの著作権、所有権などの侵害を防ぐ様にする「データハイディング」の研究が、最近活発に行われているが、これまでの処、効果的なデータハイディング技術は開発されていない。

【0005】特に、最近盛んに活用され、商業化されている、MIDI (Music Instrumental Digital Interface) の規格により構成されているMIDI音楽デジタルデータに関しては、従来から上記問題の発生を防止する為の有効な方法或いは装置は、全く開発されていないのが現状である。更に、デジタルデータ著作物等のデジタルデータに必要なセキュリティデータを埋め込む場合に、従来の方式では、デジタルコンテンツに著作者名等の著作者情報を記録するデータエリアが規定されているので、当該エリアの場所が確認出来る様に当該セキュリティデータを書き換えられてしまうと言う問題があり悪意を持つ者の手によって当該著作者情報が消失すると言う欠点があった。

【0006】つまり、当該セキュリティデータをデジタルデータに埋め込んだ場合に、そのセキュリティデータを埋め込んだであると言う情報そのものも高い秘密性を有していなければならないが、従来の方式では、係る問題点を完全に解決するに至っていないのが現状である。又、当該セキュリティデータをデジタルデータに埋め込んだ場合に、当該セキュリティデータが、容易に改ざんされる事がない様な対改ざん性を有している事も必要である。

【0007】例えば、当該セキュリティデータが埋め込まれている位置が判明してしまうと、第三者が容易にその位置で当該デジタルデータを変更してしまい、著作者データが消えてしまう可能性がある。例えば、当該セキュリティデータ埋め込みビット部分をわざと人為的にばらつかせたりわざと同じビット値に揃える様な操作を行う事によって、当該デジタルデータ著作物の本質には大きな影響を与えずにセキュリティデータのみを消去する事が出来ることにもなる。

【0008】一方、係るセキュリティデータ埋め込みデジタルデータに於いては、当該セキュリティデータが埋め込まれている事を高い確立で正確に判断出来る事

が必要であり、つまり高い証拠性が要求されるものであるが、従来の方式では、セキュリティデータが埋め込まれていないのに、セキュリティデータが埋め込まれていると間違えて判断する確立と、セキュリティデータが埋め込まれているのに、セキュリティデータが埋め込まれていないと間違えて判断する確立が高くなっており、正確性に劣るものであった。

【0009】

【発明が解決しようとする課題】本発明の目的は、上記した従来技術の欠点を改良し、簡易な技術構成に基づき、予め所定のデジタルデータ著作物に著作権を有している者、又はそのライセンスを得ている者が、自己の製品であることを後でチェックする事が出来るセキュリティデータを当該デジタルデータ著作物に予め埋め込み、それによって、自己の製品か否かの判断、不正にコピーされたものであるか否かの判断等が、後日容易に行う事の出来るデジタルデータ著作物の処理方法及びデジタルデータ著作物処理装置を提供するものである。

【0010】

【課題を解決するための手段】本発明は上記した目的を達成するため、基本的には以下に記載されたような技術構成を採用するものである。即ち、本発明にかかる第1の態様としては、デジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティデータを埋め込むに際し、当該デジタルデータ著作物を構成するデジタルデータ群から少なくとも1つのパラメータを選択し、当該選択されたパラメータに於て、当該パラメータを構成する当該デジタルデータから、予め定められた規則に従って、当該セキュリティデータを埋め込むビット位置を当該パラメータが配列されている時間軸若しくは走査方向軸に沿って順次選択抽出した後、当該選択抽出された個々のビットのそれぞれに対して、当該埋め込むべきセキュリティデータを構成するビット列の各ビットデータを順次に埋め込むデジタルデータ著作物の処理方法であり、又本発明にかかる第2の態様としては、デジタルデータ著作物記憶手段、セキュリティデータ記憶手段、当該デジタルデータ著作物記憶手段に記憶されているデジタルデータ著作物のデジタルデータからパラメータを選択するパラメータ選択手段、当該選択されたパラメータから予め定められた規則に従ってセキュリティデータを埋め込むビット位置及びそのデータ値を抽出する埋め込み位置及び埋め込みデータ抽出手段、セキュリティデータを埋め込むに際してのアルゴリズムを記憶するアルゴリズム記憶手段、当該セキュリティデータ記憶手段から抽出された個々のセキュリティデータに対して固定ビットパターン及びエラー検出ビットを付加するデータ付加手段、当該データ付加手段から出力されるセキュリティデータのビット列から個々のビット値を抽出するセキュリティデータビットデータ抽出手段、当該埋め込み位置及び埋め込みデータ抽出手段

によって抽出された当該セキュリティーデータを埋め込むべきビット位置群及びビットデータに対して、当該セキュリティーデータビットデータ抽出手段からの情報に応答して、当該アルゴリズム記憶手段に記憶されたアルゴリズムに従って、所定のセキュリティーデータビット値が埋め込まれる様に埋込処理を実行するセキュリティーデータ埋め込み手段、及び当該セキュリティーデータを埋め込んだデジタルデータ著作物を出力するデジタルデータ著作物出力手段とから構成されているデジタルデータ著作物の処理装置である。

【0011】又、本発明に係る第3の態様としては、デジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティーデータを埋め込むに際し、セキュリティーデータを埋め込むべきデジタルデータ著作物を用意する第1の工程、当該デジタルデータ著作物を構成するデジタルデータ群の中から少なくとも1つのパラメータを選択する第2の工程、当該選択されたパラメータを構成する当該デジタルデータ群から、予め定められた規則に従って、当該セキュリティーデータを埋め込むべきビット位置群を当該パラメータが配列されている時間軸若しくは走査方向軸に沿って順次選択抽出する第3の工程、当該セキュリティーデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ群を当該ビット位置群のビットデータを記憶する第4の工程、予め定められたセキュリティーデータを用意する第5の工程、当該セキュリティーデータに対して予め定められた固定ビットパターン及びエラー検出ビットを付加する第6の工程、当該固定ビットパターン及びエラー検出ビットを含むセキュリティーデータのビット列から個々のビットデータを順次選択する第7の工程、当該セキュリティーデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ群を当該ビット位置群のビットデータに対して、当該選択された個々のセキュリティーデータのビット列のビットデータに当該セキュリティーデータビット値が埋め込まれる様に埋込処理を実行する第8の工程、及び当該埋込処理され所定のセキュリティーデータビット値が埋め込まれデジタルデータ著作物を出力する第9の工程、とから構成されているデジタルデータ著作物の処理方法をコンピュータに実行させる為のプログラムを記録した記録媒体である。

【0012】又、本発明に係る第4の態様としては、セキュリティーデータが埋め込まれたデジタルデータから当該埋め込まれている当該セキュリティーデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択し、当該パラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、順次に且つ予め定められた規則に従って当該デジタルデータから所定のビットデータ群を抽出する第1の工程、当該選択抽出された当該ビットデータ群を当該ビットデータ群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換する第2の工程、当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較し両者が一致するか否を判断する第3の工程、両者が一致した場合に、当該一致したセキュリティーデータを出力する第4の工程、両者が一致しない場合に、当該一致したセキュリティーデータを出力する第5

工程からなるビットデータ群を抽出した後、当該選択抽出された当該ビットデータ群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換後、当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較判定し、両者が一致したセキュリティーデータを出力する様に構成されているデジタルデータ著作物処理方法であり、本発明に係る第5の態様としては、セキュリティーデータが埋め込まれているデジタルデータ著作物を格納しているデジタルデータ著作物記憶手段、セキュリティーデータ記憶手段、当該デジタルデータ著作物記憶手段に記憶されているセキュリティーデータが埋め込まれているデジタルデータ著作物のデジタルデータから予め定められたパラメータを選択するパラメータ選択手段、当該選択されたパラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、予め定められた規則に従って当該デジタルデータからビットデータ群を順次に選択抽出するデータ抽出手段、セキュリティーデータを埋め込むに際してのアルゴリズムを記憶するアルゴリズム記憶手段、当該データ抽出手段から抽出された個々の当該ビットデータ群を当該ビットデータ群に、当該アルゴリズムを適用して新たなビットデータ値列に変換するデータ変換手段、当該新たなビットデータ値列を、予めセキュリティーデータ記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較判定する手段、及び両者が一致した場合に、一致したセキュリティーデータを出力するセキュリティーデータ出力手段とから構成されているデジタルデータ著作物処理装置である。

【0013】更に、本発明に係る第6の態様としては、セキュリティーデータが埋め込まれたデジタルデータから当該埋め込まれている当該セキュリティーデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択する第1の工程、当該選択されたパラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、順次に且つ予め定められた規則に従って当該デジタルデータから所定のビットデータ群を抽出する第2の工程、当該選択抽出された当該ビットデータ群を当該ビットデータ群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換する第3の工程、当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較し両者が一致するか否を判断する第4の工程、両者が一致した場合に、当該一致したセキュリティーデータを出力する第5

の工程、とから構成されているデジタルデータ著作物の処理方法をコンピュータに実行させる為のプログラムを記録した記録媒体である。

【0014】

【発明の実施の形態】本発明に係るデジタルデータ著作物の処理方法及びデジタルデータ著作物処理装置は、上記したような技術構成を採用しているため、所定のデジタルデータ著作物に対して、人間の聴覚に影響の無い形式で特定のセキュリティデータ、例えば暗号データ、署名データ等を当該必要なデジタルデータ著作物に埋め込む事が出来、又容易にそれを再生する事が可能となるのである。

【0015】つまり、本発明に於いては、画像データ或いは音楽データを含むデジタルデータ著作物の様に、一般に大量のデジタルから構成される著作物に於いては、それぞれの特性を表すデジタルデータのある特定のパラメータを選択して、当該選択されたパラメータに於ける所定の選択されたデジタルデータビット若しくはデジタルデータビット群に、所定のセキュリティデータを示す所定のビットデータを埋め込んで置換しても、全体的に再生した場合には、その違和感が顕出される事が少ない事をうまく利用したものである。

【0016】然も、本発明に於いては、後述する様に、必要なセキュリティデータを第3者には判りにくいアルゴリズムを使用して、特定の変換を行い、その結果を利用して、当該デジタルデータ著作物の必要な部分に、セキュリティデータを埋め込む様にしているため、その第3者にとっては、セキュリティデータが埋め込まれているか否かを識別する事が極めて困難であると同時に、例えば、当該デジタルデータ著作物が、第3者によって改造され、折角埋め込んだセキュリティデータが一部破壊されたとしても、相当の確率を持って当該セキュリティデータを復元出来る、データ誤りに強いセキュリティデータ埋め込み方法を得る事が可能となるのである。

【0017】

【実施例】以下に、本発明に係るデータ処理方法及びデータ処理装置の具体例を図面を参照しながら詳細に説明する。即ち、図1は、本発明に係るデジタルデータ著作物処理装置100の1具体例の構成を示すブロックダイアグラムであり、図中、デジタルデータ著作物記憶手段1、セキュリティデータ記憶手段7、当該デジタルデータ著作物記憶手段1に記憶されているデジタルデータ著作物のデジタルデータからパラメータを選択するパラメータ選択手段2、当該選択されたパラメータから予め定められた規則に従ってセキュリティデータを埋め込むビット位置或いはビット位置群及びそのデータ値を抽出する埋め込み位置及び埋め込みデータ抽出手段3、セキュリティデータを埋め込むに際してのアルゴリズムを記憶するアルゴリズム記憶手段4、当該セキュリティ

データ記憶手段7から抽出された個々のセキュリティデータに対して固定ビットパターン及びエラー検出ビットを付加するデータ付加手段8、当該データ付加手段8から出力されるセキュリティデータのビット列から個々のビット値を抽出するセキュリティデータビットデータ抽出手段9、当該埋め込み位置及び埋め込みデータ抽出手段3によって抽出された当該セキュリティデータを埋め込むべきビット位置或いはビット位置群及びビットデータに対して、当該セキュリティデータビットデータ抽出手段9からのセキュリティデータ情報に応答して、当該アルゴリズム記憶手段4に記憶されたアルゴリズムに従って、所定のセキュリティデータビット値が埋め込まれる様に埋込処理を実行するセキュリティデータ埋め込み手段5、及び当該セキュリティデータを埋め込んだデジタルデータ著作物を出力するデジタルデータ著作物出力手段6及び当該セキュリティデータを埋め込んだデジタルデータ著作物を記憶させておくセキュリティデータ埋込みデジタルデータ著作物記憶手段10とから構成されているデジタルデータ著作物の処理装置100が示されている。

【0018】尚、当該デジタルデータ著作物処理装置100には、図示されていないが、更に後述するデータ処理上で同期をとる為の同期固定ビット検出手段及び検査ビット処理手段が設けられており、係る同期固定ビット検出手段及び検査ビット処理手段は、周知の構成を採用するものであり、此処ではその説明を省略する。本発明に於ける当該デジタルデータ著作物処理方法は、上記した様な構成を有するデジタルデータ著作物処理装置100を使用して、例えば、基本的には、以下の様な方法で実現する事が出来る。

【0019】即ち、デジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティデータを埋め込むに際し、当該デジタルデータ著作物を構成するデジタルデータ群から少なくとも1つのパラメータを選択し、当該選択されたパラメータに於て、当該パラメータを構成する当該デジタルデータから、予め定められた規則に従って、当該セキュリティデータを埋め込むビット位置を当該パラメータが配列されている時間軸若しくは走査方向軸に沿って順次選択抽出した後、当該選択抽出された個々のビットのそれぞれに対して、当該埋め込むべきセキュリティデータを構成するビット列の各ビットデータを順次に埋め込む様に構成されたデジタルデータ著作物の処理方法である。

【0020】本発明に於ける当該デジタルデータ著作物処理方法に於いて対象とする当該デジタルデータ著作物は、静止画像データ或いは動画画像データのいずれかであっても良く、又当該デジタルデータ著作物は、音楽データであっても良い。更に、本発明に於いては、当該音楽データは、MIDI (Music Instrumental Digital Interface) の規格により構成されているデータである事が

望ましい。

【0021】又、本発明に於ける特徴的な技術としては、当該デジタルデータ著作物を構成するデジタルデータ群から一つのパラメータが選択され、当該選択されたパラメータを構成するデジタルデータのビット列から、当該パラメータを構成する各デジタルデータが配置されている時間軸若しくは走査方向軸に沿って、予め定められた規則に従って、当該セキュリティデータを埋め込むべきビット位置或いはビット位置群を選択抽出する点にある。

【0022】本発明に係るデジタルデータ著作物処理方法の好ましい具体例を説明するならば、本発明に於いては、当該デジタルデータ著作物を構成するデジタルデータ群から複数種類のパラメータが選択され、当該時間軸若しくは走査方向軸に沿って、当該セキュリティデータを埋め込むビット位置を当該選択された複数種のパラメータ間で変化させるものであり、更に好ましい具体例としては、当該時間軸若しくは走査方向軸に沿って、当該セキュリティデータを埋め込むビット位置を選択抽出するに際して、予め定められた規則に従って、当該選択された複数種のパラメータ群の中から一つのパラメータを当該時間軸若しくは走査方向軸に沿って順次を選択すると共に、各選択されたパラメータにおいても、当該時間軸若しくは走査方向軸に沿ってビット位置或いはビット位置群が順次を選択されるものである。

【0023】つまり、本発明に於ける当該デジタルデータ著作物処理方法に於いては、当該選択された当該セキュリティデータを埋め込むべきビット位置或いはビット位置群に、当該セキュリティデータを構成するビット列の所定のビット値が埋め込まれるものである。一方、本発明に於ける当該デジタルデータ著作物処理方法に於いては、当該セキュリティデータを構成するビット列の所定のビット値を当該選択されたパラメータに於ける予め選択抽出された、複数のビット列で構成されたパラメータデータ部に対して埋め込むに際し、当該パラメータデータ部を予め定められたアルゴリズムに従って埋込処理するものである。

【0024】以下に上記した本発明に係るデジタルデータ著作物処理方法のより詳細な具体例を図面を参照しながら詳細に説明する。先ず本発明に使用されるセキュリティデータのデータ構成としては特に限定されるものではないが、図5(A)に示す様にデータ処理上の同期を採る為、及び前記した様に、セキュリティデータが埋込まれていないのにセキュリティデータが埋込まれていると誤判断される場合、或いはセキュリティデータが埋込まれているのに埋込まれていないと誤判断される場合を回避する為に使用される固定ビットパターン部51と著作者の名前、出版社の名前等或いは特殊の暗号データ等からなるセキュリティデータを示すデータビット部52及び使用されるデータに誤りがないかどうか

を検査する為のエラー検出ビット部53の3種の部分から構成されている事が望ましい。

【0025】当該セキュリティデータ部全体が例えば48ビットで構成され、固定ビットパターン部51は16ビット、データビット部52は24ビット及びエラー検出ビット部53は8ビットで構成されるものである。各部分のビット数は上記具体例に限定されるものではなく、特に固定ビットパターン部51は誤判断を避け、セキュリティデータが含まれているという判断の正確性を向上させる為には、ビット数は多い方が良い。

【0026】次に、本発明に於いては、デジタルデータ著作物の所定のデジタルデータに、当該セキュリティデータを構成する各ビットの値を順次埋込んで行くものであるが、本発明に於いては、係るデジタルデータ著作物を構成する幾つものパラメータの内から予め定められたパラメータを少なくとも一つ、好ましくは複数種を選択し、当該選択されたパラメータのそれぞれを構成する時間軸方向に或いは走査方向軸方向に連続して配列されている複数のデジタルデータの一部に、所定のセキュリティデータを構成するビットデータのの一つを埋込む様にするものである。

【0027】本発明に於ける当該パラメータとしては、例えば、当該デジタルデータ著作物が、多色画像（静止画及び動画の何れをも含む）である場合、当該画像データを構成するデジタルデータは、赤色に関連するデータ（Rデータ）群、緑色に関連するデータ（Gデータ）群及び青色に関連するデータ（Bデータ）群に区分されて走査方向軸に沿って配列されている。

【0028】従って、この場合には、当該パラメータとしては、上記した3色のデータのそれぞれを一つのパラメータとして採用する事が可能である。係るパラメータでは、通常各パラメータのデータ値は、256段階のデータ値の一つを採る事になる。又、当該デジタルデータ著作物が、音楽である場合、当該音楽データを構成するデジタルデータは、演奏する楽器毎に時間軸方向に沿って配列されている。

【0029】従って、この場合には、当該各楽器毎のデジタルデータ群を一つのパラメータとして採用する事が出来る。さらに、当該デジタルデータ著作物が、音楽である場合、当該音楽データが特にMIDIデータである場合、当該MIDIデータを構成するデジタルデータは、例えば、強度（ベロシティ）、音階、長さ（音符長）、タイミング、等のタイトルに区分されて、時間軸方向に沿って配列されている。

【0030】従って、この場合には、当該各タイトルのデジタルデータ群を一つのパラメータとして採用する事が出来る。尚、係る音楽に関連する各パラメータでは、通常各パラメータのデータ値は、128段階のデータ値の一つを採る事になる。そこで、上記したデジタルデータ著作物が画像データで、当該画像に所定のセキュリテ

ィーデータのビット列の構成する各ビット値を順次に当該画像データに埋込む場合の処理の例を以下に説明する。

【0031】今、当該画像データに埋込むべきセキュリティデータのビット列が例えば図5（B）に示す様な構成であったとする。上記した様に、本発明に於いては、当該デジタルデータ著作物を構成するデジタルデータをグループ化している幾つかのパラメータの内から、少なくとも一つのパラメータを選択するものであり、従って、選択されるパラメータは一つであっても良く、当該パラメータが複数種存在する場合には、2種のパラメータを選択しても良く、3種あるいはそれ以上のパラメータを選択する事も可能である。

【0032】そこで、今、当該デジタルデータ著作物（画像）の3色の色別の各データ群をパラメータとした場合に、その内の一つのパラメータを選択する場合について説明する。つまり、当該画像データを3種のパラメータに区分して表示したデータリストは、図3に示す様になる。

【0033】次に、パラメータ選択手段を使用して当該3種のパラメータからパラメータ2、つまりGデータを選択したとする。その後、当該パラメータ2を構成する走査軸方向に配列されているデジタルデータのデータ列から、当該セキュリティデータを埋込むべき所望のデジタルデータ位置を抽出する事になる。

【0034】係るデジタルデータの抽出は、特に限定されないが、第3者に、セキュリティデータを埋込むデータ位置として、如何なる順番に選択されているかが容易に判断される様な選択アルゴリズムは避ける事が望ましい。従って、例えば、乱数システムを導入する等して、複雑な選択抽出アルゴリズムを採用する事が望ましい。

【0035】図3の例では、当該パラメータ2のデータ列に於いて、データ位置（A）、データ位置（B）、データ位置（C）、データ位置（D）・・・が、予め定められた当該規則、つまりアルゴリズムに従って選択抽出される例を示している。そこで、先ずデータ抽出手段によってデータ位置（A）にあるデジタルデータが、当該セキュリティデータをセキュリティデータビット列の第1番目のビット値である1を埋込む位置として選択された事になる。

【0036】その後、当該埋込操作実行手段、つまり埋込み手段に於いて、当該選択されたデータ位置（A）にあるデジタルデータに、埋込みアルゴリズム記憶手段に記憶されている埋込みアルゴリズムを使用して、当該セキュリティデータをセキュリティデータビット列の第1番目のビット値である1を埋込む操作が実行される。

【0037】最も簡単な埋込み方法としては、当該セキュリティデータをセキュリティデータビット列の第

1番目のビット値である1を、当該第1番目に選択されたデータ位置（A）にあるデジタルデータのビット列の予め定められた何れかの桁に上書きする事である。つまり、予め定められた桁が、1桁目と言う様に規則化してあるとすれば、当該選択されたデータ位置（A）にあるデジタルデータの1桁目のデータ1にセキュリティデータビット列の第1番目のビット値である1が上書きされる事になる。

【0038】この場合には、表面的にはデータの変更は微小であり、聴覚、視覚的には気づかない。次に、第2番目に選択されたデータ位置（B）にあるデジタルデータの1桁目のデータ1にセキュリティデータビット列の第2番目のビット値である0が上書きされる事になる。

【0039】同様に第3番目に選択されたデータ位置（C）にあるデジタルデータの1桁目のデータ0にセキュリティデータビット列の第3番目のビット値である1が上書きされる事になる。係る操作が、図5（B）に例示された一つのセキュリティデータのデータビット列の各ビット値について順次に繰り返される事になる。

【0040】同様の操作が、又別のデータ位置から繰り返される事になる。係る操作が終了して、当該セキュリティデータを埋め込むべきデジタルデータ著作物に所定のセキュリティデータを複数箇所に埋め込んだ後は、当該デジタルデータ著作物データを適宜の媒体に出力すると共に、適宜の記憶手段に記憶させておくものである。

【0041】係るデジタルデータ著作物処理方法に於ける埋込みアルゴリズムに於いては、単にデジタルデータの1桁をセキュリティデータを構成する一つのビット値で置き換えるものである為、悪意のある第3者に容易に改ざんされやすく、又データが何らかの原因で変動した場合に誤ったデータとして判断される場合がある。その為、本発明に於いては、より複雑な埋込みアルゴリズムを採用する事が望ましく、例えば、当該アルゴリズムとして、当該パラメータを構成するデジタルデータを当該デジタルデータの通常の変化の量よりも広い間隔で量子化する方法を採用する事も望ましい。

【0042】かかる方法のより具体的な方法としては、例えば、モジュロX（X=任意の整数）方式を採用するものである。上記した具体例について、当該埋込みアルゴリズムとして、モジュロ10を採用した場合のデジタルデータ著作物処理方法の具体例を以下に説明する。今、説明を簡素化する為に、データの表示を10進法で表した場合について説明するが、勿論、当該デジタルデータ著作物処理装置に於けるコンピュータ処理上では、2進法によるデータが取り扱われる事は言うまでもない。

【0043】つまり、当該図3に於ける当該パラメータ2のデータ列に於けるデータ位置（A）、データ位置

(B)、データ位置(C)、データ位置(D)、データ位置(E)・・・の各ビットデータ値が図4に示す様な10進法によるデータを示していたとする。そして、モジュロ10を採用する場合、セキュリティデータの埋込むべきビットデータ値が1の場合に、当該パラメータのデータ値を10で割って余りが0となる様なデジタルデータ値に書き直し、セキュリティデータの埋込むべきビットデータ値が0の場合に、当該パラメータのデータ値を10で割って余りが5となる様なデジタルデータ値に書き直しをする様なアルゴリズムとなる。

【0044】従って、図4に示す様に、当該パラメータに於けるデータ位置(A)、データ位置(B)、データ位置(C)、データ位置(D)、データ位置(E)の各データ値、がそれぞれ125、127、103、117、133であったとすると、係る各データ値に対して、当該各データに埋込むべきセキュリティデータのデータビット列の各ビット値が、図5(B)に示す様に、それぞれ1、0、1、0、1・・・であるから、当該パラメータの各データ位置のデータ値は、当該モジュロ10のアルゴリズムを採用する事によって、図4の最右欄に示す様にデータ位置(A)、データ位置(B)、データ位置(C)、データ位置(D)、データ位置

(E)の各データ値は、120、125、100、115、130という様に書換えられる事になる。

【0045】係る変換結果は当然2進法によるバイナリデータとして変換されるものであり、その結果は、バイナリデータとしてデジタルデータ著作物に埋込まれる事になる。かかる埋込みアルゴリズムを採用する事によって、仮にデータが1つ変化した場合でも何方かに近い法のデータであると判断して処理する事が可能であるので、前記した具体例よりも誤りの判断をする確立は大きく減少する事になる。

【0046】つまり、例えば、デジタルデータ著作物のパラメータのデータ値が何らかの理由で変動した事によって、当該パラメータのデジタルデータを10で割った値が1、2、8、又は9である場合には、当該デジタルデータは、10で割り切れるデータ値であると判断し、又その余りが3、4、5又は6である場合には、当該デジタルデータは、10で割った場合に余りが5となるデータ値であると判断するものである。

【0047】本具体例に於いては、モジュロ10以外の例えばモジュロ2以上任意のモジュロ値を採用する事が可能であるが、モジュロ2では、データの変動に対してデータの判断を誤る確立が高い点を注意する必要がある。上記した具体例の基本的な考え方は、以下の通りである。即ち、当該デジタルデータ著作物処理装置100が、上記したエンコード機能を利用して当該セキュリティデータ情報を埋め込んだ後、デジタルコンテンツを編集する事で当該セキュリティデータを埋込んだパラメータ値が変化し、それによって当該エンコードが埋込

んだ時の、パラメータ値とデコーダが読み込んだパラメータとが変化した場合に、それでも当該セキュリティデータ情報が正しく検出できる様にすることが必要である。

【0048】即ち、当該編集等に伴うパラメータ変動値よりも広い間隔で当該パラメータ値を量子化し、当該量子化によって離散的になったパラメータ値によってセキュリティデータ情報を表わす事が望ましい。例えば、データの変動量を y とした場合に当該変動後のパラメータ値 p_d は、

元のパラメータ値 $-y \leq p_d \leq$ 元のパラメータ値 $+y$ の範囲に収まる。

【0049】今、当該セキュリティデータ情報を埋込む場合のエンコード時のパラメータ値を p_e とし、当該パラメータ p_e を x の幅で量子化する。ここで、 $x \geq 2y$ とする。ここで、例えば、当該セキュリティデータ情報の各ビット値0を埋込む場合には、当該パラメータ値 p_e を $x/2$ の偶数倍の値に書き換え、当該セキュリティデータ情報のビット1を埋込む場合には、当該パラメータ値 p_e を $x/2$ の奇数倍の値に書き換える。

【0050】デコード時には、読み取りパラメータ値 p_d が $x/2$ の偶数倍と奇数倍とで偶数倍に近ければ埋込まれたセキュリティデータ情報のビット値は0であると判断し、奇数倍に近ければ、当該埋込まれたセキュリティデータ情報のビット値は1であると判断する。即ち、デコード前にパラメータ値が $+y$ から $-y$ まで変動したとしても、正しくセキュリティデータ情報のビット値を検出する事が可能となる。

【0051】つまり、本発明に係る上記したデジタルデータ著作物処理方法を採用する事によって、デジタルコンテンツの内容そのものであるデータ要素にセキュリティデータ情報を秘密裏に重畳する事によって、一見してどこにもセキュリティデータが重畳されているかを認識出来ず、又デジタルコンテンツを破壊することなく、当該セキュリティデータ情報を消し去る事が不可能となり、よって、強固且つ不可視的にセキュリティデータを重畳してセキュリティデータが消失する事を効果的に防止することが可能となる。

【0052】次に、本発明に係る当該デジタルデータ著作物処理方法の他の具体例について説明するならば、上記した具体例は何れも当該デジタルデータ著作物に関して一つのパラメータしか選択しない例について説明したものであるが、本発明に於いて複数種のパラメータを選択する場合を以下に説明する。つまり、上記した具体例と同様に当該セキュリティデータを埋込むべきデジタルデータ著作物が、カラー画像である場合に、図6に示す様に3種のパラメータが存在するので、当該3種のパラメータから2種或いは3種を選択する事が可能である。

【0053】今、当該パラメータとして3種のパラメー

タつまり第1のパラメータ(Rデータ)群、第2のパラメータ(Gデータ)群及び第3のパラメータ(Bデータ)群の全てのパラメータを選択するとする。係る具体例では、上記した具体例に於ける一つのパラメータに於けるデータ列の時間軸若しくは走査方向軸の選択規則に加えて、3種のパラメータの内のどのパラメータを如何なる時間若しくは走査タイミングでそれぞれ選択するかのパラメータ選択に関する別の選択埋込みアルゴリズムが必要となる。

【0054】係るパラメータの選択方法と各パラメータに於けるデータの選択方法とは任意に組み合わせる事が可能であり、第3者に判らない様に適宜乱数システム等を導入する事によってより複雑な選択埋込みアルゴリズムを採用する事が望ましい。図6では単にその一例として、当該各データに埋め込むべきセキュリティデータのデータビット列の各ビット値が、図5(B)に示す様に、それぞれ1、0、1、0、1、1、0、1・・・に対して、パラメータ2の(a)位置、パラメータ1の(b)位置、パラメータ3の(c)位置、パラメータ1の(d)位置、パラメータ2の(e)位置、パラメータ1の(f)位置、パラメータ3の(g)位置に有る各データが選択される例を示している。

【0055】係る選択埋込みアルゴリズムは、任意に選定する事が可能である。又、当該各選択された各パラメータのデータ値に当該セキュリティデータの所定のビット値を埋め込む方法は、上記した何れかの方法を任意に採用する事によって実行されるものである。係るセキュリティデータの埋込み方法は、当該デジタルデータ著作物が音楽データである場合に於いても同様である。

【0056】但し、当該デジタルデータ著作物が音楽であって、当該デジタルデータ著作物のパラメータが、楽器毎に区分されている場合に、例外的に一つのパラメータ内でデータの範囲に応じて異なる楽器のデータを取扱場合がある。係る場合に、例えば上記したモジュロXによる埋込みアルゴリズムを採用する場合には、一方の楽器に関するデータを変換処理した後のデータが、他の楽器を取扱データの範囲内のデータにならない様に注意をする必要がある。

【0057】上記した本発明に係るデジタルデータ著作物処理方法の操作手順を纏めて図2に示す様なフローチャートを参照して説明する。即ち、スタート後、ステップ(1)に於いてデジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティデータを埋め込むに際し、セキュリティデータを埋め込むべきデジタルデータ著作物を用意する第1の工程が実行され、次いでステップ(2)に移り、当該デジタルデータ著作物を構成するデジタルデータ群の中から少なくとも1つのパラメータを選択する第2の工程が実行される。

【0058】その後、ステップ(3)に進み、当該選択されたパラメータを構成する当該デジタルデータ群か

ら、予め定められた規則に従って、当該セキュリティデータを埋め込むべきビット位置或いはビット位置群からなるデータ位置を当該パラメータが配列されている時間軸若しくは走査方向軸に沿って順次選択抽出する第3の工程が実行され、ステップ(4)で、当該セキュリティデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ或いは選択された当該データ位置と当該データ位置に於けるビットデータを記憶する第4の工程が実行される。

【0059】その後、ステップ(5)で、予め定められたセキュリティデータを用意する第5の工程を実行した後、ステップ(6)に進み、当該セキュリティデータに対して予め定められた固定ビットパターン及びエラー検出ビットを付加する第6の工程が実行される。次いで、ステップ(7)に於いて、当該固定ビットパターン及びエラー検出ビットを含むセキュリティデータのビット列から個々のビットデータを順次を選択する第7の工程が実行された後に、ステップ(8)に移り、当該セキュリティデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ或いは選択されたビット位置群のビットデータに対して、当該選択された個々のセキュリティデータのビット列のビットデータに応答して、当該アルゴリズムを介して、所定のセキュリティデータビット値が埋め込まれる様に埋込処理を実行する第8の工程が実行される。

【0060】その後、ステップ(9)に於いて、当該埋込処理され所定のセキュリティデータビット値が埋め込まれデジタルデータ著作物を出力する第9の工程が実行され、その後必要に応じてステップ(10)に於いて、当該セキュリティデータビット値が埋め込まれデジタルデータ著作物を所定の記憶手段に記憶させておく操作が実行されてエンドとなる。

【0061】本発明に於ける当該第9の工程に於ける出力の具体例としては、適宜の媒体、例えば、印刷処理、磁気テープ、CD、MD等の媒体に出力される事になる。次に、本発明に係るセキュリティデータを埋込んだデジタルデータ著作物から当該埋込まれたセキュリティデータを読み出す為のデジタルデータ著作物処理方法について説明する。

【0062】即ち、上記した方法によって、所定のデジタルデータ著作物に所定のセキュリティデータが埋込まれている当該デジタルデータ著作物から当該埋込まれているセキュリティデータ情報を読み出すに際し、本発明に於いては、基本的には、セキュリティデータが埋め込まれたデジタルデータから当該埋込まれている当該セキュリティデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択し、当該パラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、順次に且つ予め定

められた規則に従って当該デジタルデータから所定のビットデータ或いは複数のビットデータからなるビットデータ群を抽出した後、当該選択抽出された当該ビットデータ或いは当該ビットデータ群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換後、当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較判定し、両者が一致したセキュリティーデータを出力する様に構成されているデジタルデータ著作物処理方法を採用するものである。

【0063】上記したデジタルデータ著作物処理方法を実行する為のデジタルデータ著作物処理装置200の例としては、図7に示す様に、セキュリティーデータが埋め込まれているデジタルデータ著作物を格納しているデジタルデータ著作物記憶手段20、セキュリティーデータ記憶手段7、当該デジタルデータ著作物記憶手段20に記憶されているセキュリティーデータが埋め込まれているデジタルデータ著作物のデジタルデータから予め定められたパラメータを選択するパラメータ選択手段2、当該選択されたパラメータを構成する各デジタルデータが配列されている時間軸若しくは走査方向軸に沿って、予め定められた規則に従って当該デジタルデータからビットデータ或いは複数のビットデータからなるビットデータ群を順次に選択抽出するデータ抽出手段3、セキュリティーデータを埋め込むに際してのアルゴリズムを記憶するアルゴリズム記憶手段4、当該データ抽出手段3から抽出された個々の当該ビットデータ或いは複数のビットデータからなるビットデータ群に、当該アルゴリズムを適用して新たなビットデータ値列に変換するデータ変換手段21、当該変換された新たなビットデータ値列を、予めセキュリティーデータ記憶手段7に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較判定する手段22、及び両者が一致した場合に、一致したセキュリティーデータを出力するセキュリティーデータ出力手段23とから構成されているものである。

【0064】当該デジタルデータ著作物処理装置200に於ける各手段の内図1に示す手段と同一の符号を付した手段は、当該図1に於けるデジタルデータ著作物処理装置100に於ける手段と同一の機能を発揮するものである。尚、当該デジタルデータ著作物処理装置200には、図示されてはいないが、更に前記したデータ処理上で同期をとる為の同期固定ビット検出手段及び検査ビット処理手段が設けられており、係る同期固定ビット検出手段及び検査ビット処理手段は、周知の構成を採用するものであり、此处ではその説明を省略する。

【0065】本具体例に於いて、当該デジタルデータ著作物記憶手段2から呼び出された所定のデジタルデータ著作物に所定のセキュリティーデータが埋め込まれている当該デジタルデータ著作物から当該埋め込まれているセキ

ュリティーデータ情報を読み出すに際し、所定の同期を採った上で、当該デジタルデータ著作物を構成するデジタルデータ群から予め定められた一つ若しくは複数種のパラメータが、当該パラメータ選択手段2によって選択する。

【0066】係る操作に於いては、前記した具体例に示す様に、如何なるパラメータを選択するかは、既に決まっているので、当該決定されているパラメータの選択情報を使用する事によって、容易に必要な選択すべきパラメータを選択する事が可能である。次いで、当該選択された一つ若しくは複数種のパラメータ群から、これも既に決定されている選択規則、選択埋込みアルゴリズムを使用する事によって、順次に当該選択された一つ若しくは複数種のパラメータの内から一つずつ順次に選択すると同時に、当該選択された各パラメータにおいて、前記した予め定められた選択規則に従って各パラメータ内で、時間軸若しくは走査方向軸に沿って配列されている所定のデータ位置にある各デジタルデータのビットデータ或いは複数のビットデータからなるビットデータ群を順次にデータ抽出手段3によって選択抽出される。

【0067】そして、当該データ抽出手段3によって選択抽出された一つのパラメータに於ける所定のデータ位置に於けるデジタルデータを当該データ変換手段21に於いて当該アルゴリズム記憶手段4に記憶されている当該埋込み埋込みアルゴリズムを使用して、当該選択抽出されたデジタルデータを解読して、当該デジタルデータに埋め込まれているセキュリティーデータを構成する一つのビットデータの値を検出しデコードするものである。

【0068】今、所定のデータ選択抽出規則、埋込みアルゴリズムに従って、所定のパラメータが選択され、当該選択されたパラメータに於ける当該データ位置(A)～(E)でのそれぞれのデータ値が10進法によって図8に示す様に、120、125、100、115、130の様に検出されたとすると、係るデータにモジュロ10の埋込みアルゴリズムを適用する事によって、当該データ位置(A)～(E)でのそれぞれのデータには、セキュリティーデータを構成するデータビット列の第1番めから第5番目までのデータである1、0、1、0、1がそれぞれ埋め込まれていた事が判明する。

【0069】その後、当該デコードされた変換データをセキュリティーデータ記憶手段7のデータと当該比較手段22で比較操作が実行され、当該デコードされた変換データが、当該セキュリティーデータ記憶手段7のセキュリティーデータと一致した場合には、その結果が適宜の出力手段を介して出力される。つまり、それによって、当該デジタルデータ著作物が、正当なデジタルデータ著作物であるか否かが判断出来るのである。

【0070】即ち、上記した本発明に係る当該デジタルデータ著作物処理方法の具体例の手順を図9に示すフロ

ーチャートを参照して説明するならば、スタート後、ステップ（１）に於いて、セキュリティーデータが埋め込まれたデジタルデータから当該埋め込まれている当該セキュリティーデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択する第１の工程が実行され、ステップ

（２）に進み、当該選択されたパラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸及び走査方向軸に沿って、順次に且つ予め定められた規則に従って当該デジタルデータから所定のビットデータ或いは複数のビットデータからなるビットデータ位置群を抽出する第２の工程が実行される。

【００７１】次いで、ステップ（３）に移り、当該選択抽出された当該ビットデータ或いは当該ビットデータからなるデータ位置群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換する第３の工程が実行された後、ステップ（４）に進み、当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較し両者が一致するか否かを判断する第４の工程が実行され、次いでステップ（５）に進み、両者が一致した場合に、当該一致したセキュリティーデータを出力する第５の工程が実行されてエンドとなる。

【００７２】尚、本発明に於ける上記データ処理操作に於いては、当該パラメータの選択する第１の工程に於いて、一つのデジタルデータ著作物のデジタルデータから複数種のパラメータを選択し、当該選択された複数種のパラメータ群の中から一つのパラメータを当該時間軸及び走査方向軸に沿って順次に選択すると同時に、当該選択されたそれぞれのパラメータを構成するデジタルデータ列から、当該時間軸及び走査方向軸に沿って予め定められた規則に従って、当該ビットデータ或いは複数のビットデータからなるビットデータのデータ位置を選択抽出する操作が実行されるものである。

【００７３】本発明に係る他の態様としては、デジタルデータにより構成されたデジタルデータ著作物に所定のセキュリティーデータを埋め込むに際し、セキュリティーデータを埋め込むべきデジタルデータ著作物を用意する第１の工程、当該デジタルデータ著作物を構成するデジタルデータ群の中から少なくとも１つのパラメータを選択する第２の工程、当該選択されたパラメータを構成する当該デジタルデータ群から、予め定められた規則に従って、当該セキュリティーデータを埋め込むべきビット位置或いはビット位置群を当該パラメータが配列されている時間軸及び走査方向軸に沿って順次選択抽出する第３の工程、当該セキュリティーデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ或いは選択されたビット位置群のビットデータを記憶する第４の工程、予め定められたセキュリティーデータを用意する第５の工程、当該セキュリティーデータに対して予め

定められた固定ビットパターン及びエラー検出ビットを付加する第６の工程、当該固定ビットパターン及びエラー検出ビットを含むセキュリティーデータのビット列から個々のビットデータを順次に選択する第７の工程、当該セキュリティーデータを埋め込む為に選択抽出されたビット位置の個々のビットデータ或いは選択されたビット位置群のビットデータに対して、当該選択された個々のセキュリティーデータのビット列のビットデータに回答して、当該アルゴリズムを介して、所定のセキュリティーデータビット値が埋め込まれる様に埋込処理を実行する第８の工程、及び 当該埋込処理され所定のセキュリティーデータビット値が埋め込まれたデジタルデータ著作物を出力する第９の工程、とから構成されているデジタルデータ著作物の処理方法をコンピュータに実行させる為のプログラムを記録した記録媒体である。

【００７４】更に本発明に係る別の態様としては、セキュリティーデータが埋め込まれたデジタルデータから当該埋め込まれている当該セキュリティーデータを読み出すに際し、当該デジタルデータ著作物処理から予め定められた少なくとも一つのパラメータを選択する第１の工程、当該選択されたパラメータから、当該パラメータを構成する各デジタルデータが配列されている時間軸及び走査方向軸に沿って、順次に且つ予め定められた規則に従って当該デジタルデータから所定のビットデータ或いは複数のビットデータからなるビットデータ群を抽出する第２の工程、当該選択抽出された当該ビットデータ或いは当該ビットデータ群を順次に予め定められたアルゴリズムを適用して、新たなビットデータ値列に変換する第３の工程、当該新たなビットデータ値列を、予め適宜の記憶手段に記憶されている所定のセキュリティーデータを表わすビットデータ値列と比較し両者が一致するか否かを判断する第４の工程、両者が一致した場合に、当該一致したセキュリティーデータを出力する第５の工程、とから構成されているデジタルデータ著作物の処理方法をコンピュータに実行させる為のプログラムを記録した記録媒体である。

【００７５】

【発明の効果】本発明に係る当該デジタルデータ著作物処理方法及びデジタルデータ著作物処理装置は、上記した様な技術構成を採用しているので、簡易な技術構成に基づき、予め所定のデジタルデータ著作物に著作権を有している者、又はそのライセンスを得ている者が、自己の製品である事を後でチェックする事が出来るセキュリティーデータを当該デジタルデータ著作物に予め埋め込み、それによって、自己の製品か否かの判断、不正にコピーされたものであるか否かの判断等が、後日容易に行う事の出来るデジタルデータ著作物の処理方法及びデジタルデータ著作物処理装置を提供するものである。

【図面の簡単な説明】

【図１】図１は、本発明に係るデジタルデータ著作物処

理装置の一具体例の構成を示すブロックダイアグラムである。

【図2】図2は、本発明に係るデジタルデータ著作物の処理方法の操作手順の一例を説明するフローチャートである。

【図3】図3は、本発明に係るデジタルデータ著作物の処理方法の一具体例に於いて使用されるパラメータの選択例を示す図である。

【図4】図4は、本発明に係るデジタルデータ著作物の処理方法の一具体例に於いて使用されるパラメータに対してセキュリティデータを埋込む操作の一例を示す図である。

【図5】図5は、本発明に係るデジタルデータ著作物の処理方法の一具体例に於いて使用されるセキュリティデータのビット列の例を示す図である。

【図6】図6は、本発明に係るデジタルデータ著作物の処理方法の一具体例に於いて使用されるパラメータの他の選択例を示す図である。

【図7】図7は、本発明に係るデジタルデータ著作物処理装置の他の具体例の構成を示すブロックダイアグラムである。

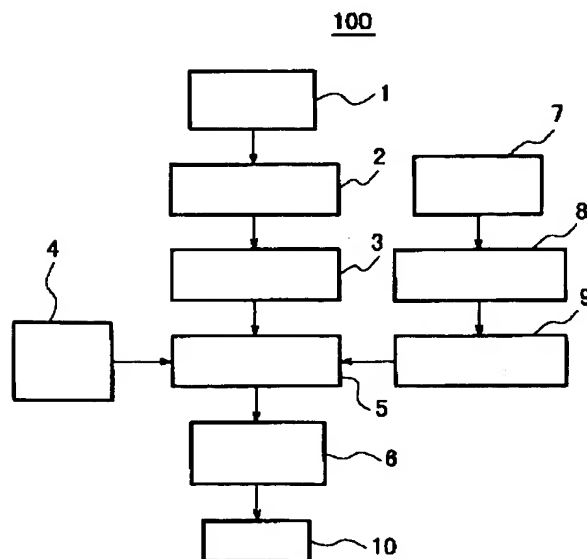
【図8】図8は、本発明に係るデジタルデータ著作物の処理方法の他の具体例に於いて使用されるパラメータのデジタルデータから埋込まれているセキュリティデータを読み出す操作の一例を示す図である。

【図9】図9は、本発明に係るデジタルデータ著作物の処理方法の操作手順の一例を説明するフローチャートである。

【符号の説明】

- 1 0 0 …デジタルデータ著作物処理装置（セキュリティデータ埋込み装置）
- 2 0 0 …デジタルデータ著作物処理装置（セキュリティデータ読出し装置）
- 1 …デジタルデータ著作物記憶手段
- 2 …パラメータ選択手段
- 3 …埋め込み位置及び埋め込みデータ抽出手段
- 4 …アルゴリズム記憶手段
- 5 …セキュリティデータ埋め込み手段
- 6 …デジタルデータ著作物出力手段
- 7 …セキュリティデータ記憶手段
- 8 …データ付加手段
- 9 …セキュリティデータビットデータ抽出手段
- 1 0 …セキュリティデータ埋込みデジタルデータ著作物記憶手段
- 2 0 …セキュリティデータ埋込みデジタルデータ著作物記憶手段
- 2 1 …データ変換手段
- 2 2 …比較判定する手段
- 2 3 …セキュリティデータ出力手段

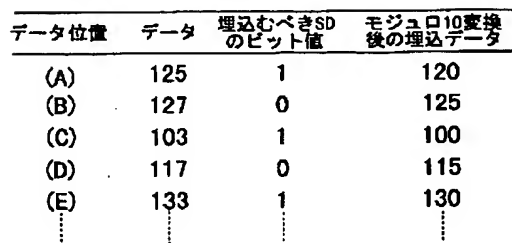
【図1】



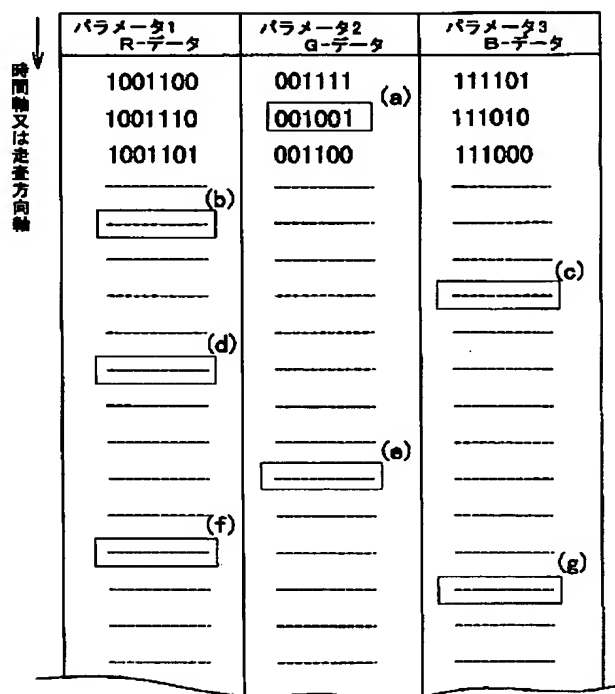
【図3】

| パラメータ1 R-データ | パラメータ2 G-データ | パラメータ3 B-データ |
|-----------------|-----------------|-----------------|
| 1001100 | 001111 (A) | 111101 |
| 1001110 | 00100① | 111010 |
| 1001101 | 001100 | 111000 |
| ----- | ----- | ----- |
| ----- | ----- (B) | ----- |
| ----- | 011001② | ----- |
| ----- | ----- (C) | ----- |
| ----- | 011100③ | ----- |
| ----- | ----- | ----- |
| ----- | ----- | ----- |
| ----- | 011001④ (D) | ----- |

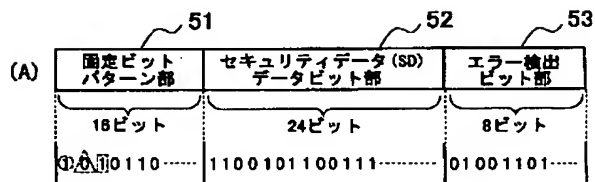
【図 4】



【図 6】



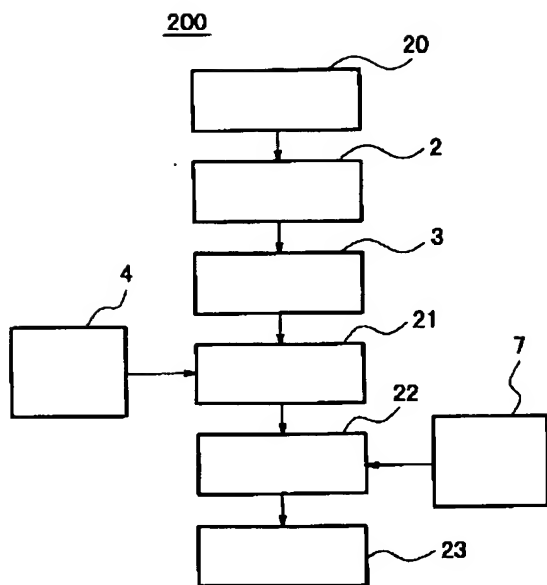
【図 5】



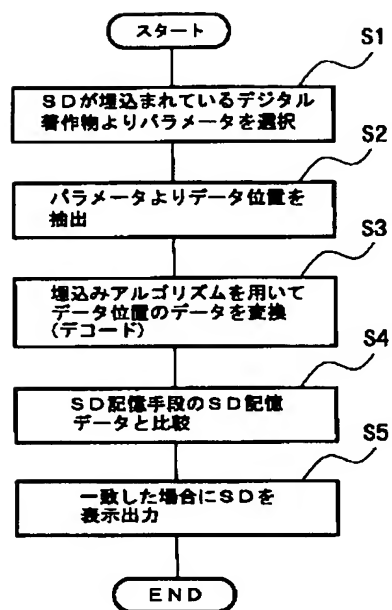
【図 8】

| 抽出データ | モジュール 変換後のデータ | SD記憶値 | 比較結果 |
|---------|------------------|-------|------|
| (a) 120 | (余り) 1 | 1 | 1 |
| (b) 125 | (余り) 0 | 0 | 0 |
| (c) 100 | (余り) 1 | 1 | 1 |
| (d) 115 | (余り) 0 | 0 | 0 |
| (e) 130 | (余り) 1 | 1 | 1 |

【図7】



【図9】



フロントページの続き

Fターム(参考) 5D044 AB05 AB06 AB07 DE50 DE52
 DE68 GK07 GK17
 5J064 AA00 BA13 BC01 BC14 BC25
 BC29 BD03